ATTACHMENT J.P-4
LEADING EDGE TECHNOLOGY DESCRIPTIONS

Artificial Intelligence (AI): Artificial intelligence (AI) is the intelligence exhibited by machines or the creation of computers and computer software that are capable of intelligent behavior. Major AI researchers and textbooks define this field as "the study and design of intelligent agents", in which an intelligent agent is a system that perceives its environment and takes actions that maximize its chances of success.

The central problems (or goals) of AI research include reasoning, knowledge, planning, learning, natural language processing (communication), perception and the ability to move and manipulate objects. General intelligence is still among the field's long-term goals. Currently popular approaches include statistical methods, computational intelligence and traditional symbolic AI. There are a large number of tools used in AI, including versions of search and mathematical optimization, logic, methods based on probability and economics, and many others. The AI field is interdisciplinary, in which a number of sciences and professions converge, including computer science, mathematics, psychology, linguistics, philosophy and neuroscience, as well as other specialized fields such as artificial psychology.

Acceptable citations must clearly include LET cited with the scope statement highlighted to indicate the activity that qualifies including – but not limited to – the list of examples below:

- AI software development
- AI software deployment
- AI systems integration
- AI systems maintenance
- AI systems security

Autonomic Computing: is a self-managing computing model named after, and patterned on, the human body's autonomic nervous system. An autonomic computing system would control the functioning of computer applications and systems without input from the user, in the same way that the autonomic nervous system regulates body systems without conscious input from the individual. The goal of autonomic computing is to create systems that run themselves, capable of high-level functioning while keeping the system's complexity invisible to the user.

Autonomic computing is one of the building blocks of pervasive computing, an anticipated future computing model in which tiny - even invisible - computers will be all around us, communicating through increasingly interconnected networks.

Acceptable citations must clearly include LET cited with the scope statement highlighted to indicate the activity that qualifies including – but are not limited to – the list of examples below:

- Pervasive computing software tools
- Autonomic solution design
- Autonomic solution integration
- “Self-healing” solutions
- Autonomic software development

Big Data: Big data is an evolving term that describes any voluminous amount of structured, semi-structured and unstructured data that has the potential to be mined for information. Big data can be characterized by 3Vs: the extreme volume of data, the wide variety of types of data, and the velocity at which the data must be processed. Although big data doesn't refer to any specific quantity, the term is often used when speaking about petabytes and exabytes of data, much of which cannot be integrated easily.

Because big data takes too much time and costs too much money to load into a traditional relational database for analysis, new approaches to storing and analyzing data have emerged that rely less on data schema and data quality. Instead, raw data with extended metadata is aggregated in a data lake and machine learning and artificial intelligence (AI) programs use complex algorithms to look for repeatable patterns.

Big data analytics is often associated with cloud computing because the analysis of large data sets in real-time requires a platform to store large data sets across a distributed cluster to coordinate, combine and process data from multiple sources.

Big data can be contrasted with small data, another evolving term that's often used to describe data whose volume and format can be easily used for self-service analytics. A commonly quoted axiom is that "big data is for machines; small data is for people."

Big data management - also considered in scope of this LET - is the organization, administration and governance of large volumes of both structured and unstructured data.

The goal of big data management is to ensure a high level of data quality and accessibility for business intelligence and big data analytics applications. Corporations, government agencies and other organizations employ big data management strategies to help them contend with fast-growing pools of data, typically involving many terabytes or even petabytes of information saved in a variety of file formats. Effective big data management helps companies locate valuable information in large sets of unstructured data and semi-structured data from a variety of sources, including call detail records, system logs, social media sites, cyber security activities, business analytics and other data application and synthesis requirements. This process requires careful data classification so that ultimately, smaller sets of data can be analyzed quickly and productively.

Acceptable citations must clearly include LET cited with the scope statement highlighted to indicate the activity that qualifies including – but are not limited to – the list of examples below:

- Big data analytics
- Big data systems integration
- Big data systems maintenance
- Big data software tools development
- Big data application/tools deployment
- Big data systems administration
- Big data management
- Big data systems security
- Big data normalization

Biometrics: Biometrics is the science and technology of measuring and statistically analyzing biological data. In information technology, biometrics usually refers to technologies for measuring and analyzing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for authentication purposes.

Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics and point of sale (POS) applications. In addition to security, the driving force behind biometric verification has been convenience.

Biometric recognition systems such as fingerprint, iris, face, voice, hand geometry, and retina, etc., consist of:

• A reader or scanning device

• Software that converts the scanned information into digital form and compares match points

• A database that stores the biometric data for comparison

To prevent identity theft, biometric data is usually encrypted when it's gathered. Here's how biometric verification works on the back end: To convert the biometric input, a software application is used to identify specific points of data as match points. The match points in the database are processed using an algorithm that translates that information into a numeric value. The database value is compared with the biometric input the end user has entered into the scanner and authentication is either approved or denied.

Acceptable citations must clearly include LET cited with the scope statement highlighted to indicate the activity that qualifies including – but are not limited to – the list of examples below:

- Biometric access systems hardware installation
- Biometric access systems hardware maintenance/support
- Multimodal biometric systems integration (unimodal or multimodal)
- Biometric systems maintenance (unimodal or multimodal)
- Biometric software development
- Biometric software maintenance & updates
- Biometric database development/maintenance/support

Cloud Computing: Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

Cloud computing enables companies to consume computer resources as a utility -- just like electricity -- rather than having to build and maintain computing infrastructures in-house. Cloud computing promises several attractive benefits for businesses and end users. Three of the main benefits of cloud computing include:

• Self-service provisioning: End users can spin up computing resources for almost any type of workload on-demand.

• Elasticity: Companies can scale up as computing needs increase and then scale down again as demands decrease.

• Pay per use: Computing resources are measured at a granular level, allowing users to pay only for the resources and workloads they use.

Cloud computing services can be private, public or hybrid.

Private cloud services are delivered from a business' data center to internal users. This model offers versatility and convenience, while preserving management, control and security. Internal customers may or may not be billed for services through IT chargeback.

In the public cloud model, a third-party provider delivers the cloud service over the Internet. Public cloud services are sold on-demand, typically by the minute or the hour. Customers only pay for the Computer Processing Unit (CPU) cycles, storage or bandwidth they consume.

Hybrid cloud is a combination of public cloud services and on-premises private cloud – with orchestration and automation between the two. Companies can run mission-critical workloads or sensitive applications on the private cloud while using the public cloud for burst workloads that must scale on-demand. The goal of hybrid cloud is to create a unified, automated, scalable environment which takes advantage of all that a public cloud infrastructure can provide, while still maintaining control over mission-critical data.

Although cloud computing has changed over time, it has always been divided into three broad service categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as service (SaaS).

IaaS providers supply a virtual server instance and storage, as well as application program interfaces (APIs) that let users migrate workloads to a virtual machine (VM). Users have an allocated storage capacity and start, stop, access and configure the VM and storage as desired. IaaS providers offer small, medium, large, extra-large, and memory- or compute-optimized instances, in addition to customized instances, for various workload needs.

In the PaaS model, providers host development tools on their infrastructures. Users access those tools over the Internet using Application Programming Interfaces (APIs), Web portals or gateway software. PaaS is used for general software development and many PaaS providers will host the software after it's developed.

SaaS is a distribution model that delivers software applications over the Internet; these are often called Web services. Users can access SaaS applications and services from any location using a computer or mobile device that has Internet access.

Work cited to enable, implement, integrate or provision any of the cloud services is considered in scope of this LET

Acceptable citations must clearly include LET cited with the scope statement highlighted to indicate the activity that qualifies including – but are not limited to – the list of examples below:

- Cloud migration planning
- Cloud migration implementation

- Cloud service provisioning
- Cloud solution security
- Cloud data migration

Cybersecurity: is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term security implies cybersecurity. To deal with the current environment, advisory organizations are promoting a more proactive and adaptive approach. The National Institute of Standards and Technology (NIST), for example, recently issued updated guidelines in its risk assessment framework that recommended a shift toward continuous monitoring and real-time assessments.

Acceptable citations must clearly include LET cited with the scope statement highlighted to indicate the activity that qualifies including – but are not limited to – the list of examples below:

- Predictive analytics
- Machine learning
- Behavioral analytics
- Real time assessment tool development
- Real time assessment tool integration
- Digital forensics
- Emergency readiness
- Systems disaster recovery
- Application security
- Device security
- Service hardening

Health Information Technology (HIT) is the application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision making. HIT "technology" can refer to material objects, such as machines, hardware or utensils, but can also encompass broader themes, including systems, methods of organization, and techniques. For HIT, technology represents computers and communications attributes that can be networked to build systems for moving health information.

Informatics is yet another integral aspect of HIT.

Informatics refers to the science of information, the practice of information processing, and the engineering of information systems. Informatics underlies the academic investigation and practitioner application of computing and communications technology to healthcare, health education, and biomedical research. Health informatics refers to the intersection of information science, computer science, and health care. Health informatics describes the use and sharing of information within the healthcare industry with contributions from computer science, mathematics, and psychology. It deals with the resources, devices, and methods required for optimizing the acquisition, storage, retrieval, and use of information in health and biomedicine. Health informatics tools information and communication systems. Medical informatics, nursing informatics, public health informatics, pharmacy informatics, and translational bioinformatics are sub disciplines that inform health informatics from different disciplinary perspectives.

Acceptable citations must clearly include LET cited with the scope statement highlighted to indicate the activity that qualifies including – but are not limited to – the list of examples below:

- Federal Health Architecture (FHA)
- Health Infomatics
- Digital record systems implementation
- Health IT application development
- Health IT application integration
- Health IT security
- Health IT Device integration

The Internet of Things (IoT) is a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS) and the Internet.

A "thing", in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network. So far, the Internet of Things has been most closely associated with machine-to-machine (M2M) communication in manufacturing and power, oil and gas utilities. Products built with M2M communication capabilities are often referred to as being smart (smart label, smart meter, smart grid sensor).

Acceptable citations must clearly include LET cited with the scope statement highlighted to indicate the activity that qualifies including – but are not limited to – the list of examples below:

- Sensor data synthesis
- Sensor implementation/integration
- Machine-to-machine communication
- Process automation

Mobile IT (mobile information technology) is the ability an information technology (IT) department has to deliver IT services to employees working on mobile devices.

While the consumer world is rapidly shifting to mobile-first delivery of information, with smart phones tablets and other mobile devices rapidly becoming the vehicle for doing everything from sending and receiving mail to depositing checks, the same transition in the business world will likely take years. Mobile IT is more than implementing a "bring your own device" (BYOD) program. Legacy applications must be redesigned to work -- and to work securely -- on mobile devices. The need to manage mobile IT has given rise to a whole new class of vendors known as mobile device management (MDM) providers. The trend has also accelerated the use of desktop virtualization to allow for secure access to enterprise applications.

Acceptable citations must clearly include LET cited with the scope statement highlighted to indicate the activity that qualifies including – but are not limited to – the list of examples below:

- Mobile application migration
- Mobile business intelligence
- Mobile application development
- Mobile device security
- "Single Pane of Glass" integration
- Mobile device management

Virtual Networking is a technology that facilitates the control of one or more remotely located computers or servers over the Internet. Data can be stored and retrieved, software can be run, and peripherals can be operated through a Web browser as if the distant hardware were onsite.

Virtual networking facilitates consolidation of diverse services and devices on a single hardware platform called a virtual services switch. The centralization of control reduces the cost and complexity of operating and maintaining hardware and software compared with administering numerous separate devices in widely separated geographical locations. Maintenance personnel and administrators can install device drivers, perform tests and resolve problems on the remote machines from a single location.

Acceptable citations must clearly include LET cited with the scope statement highlighted to indicate the activity that qualifies including – but are not limited to – the list of examples below:

- Virtual Private Network implementation
- Virtual network security
- Virtual network software tools development
- Virtual network software tools implementation